UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/625,547	07/25/2000	Laurence Hamid	12-52 US	7157

7590 08/30/2004

Gordon Freedman
Freedman & Associates
117 Centrepointe Drive
Suite 350
Nepean, ON K2G 5X3
CANADA

EXAMINER	
ZAND, KAMBIZ	

ART UNIT	PAPER NUMBER
2132	4

DATE MAILED: 08/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/625,547	HAMID ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 July 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2 and 3*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-20** have been examined.

Drawings

2. New formal drawings are required in this application because original drawings by the applicant were objected to by the Draftsperson under 37 CFR 1.84 or 1.152. Please see attached PTO-948. Correction is requested.

3. Figure 1 and 2 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Correction is requested.

4. Fig.3 and 4 consist of number of drawings. Examiner suggests fig.3 be re-named as fig.3a, 3b and 3c; and fig.4 be renamed as fig.4a,4b,4c and 4d in order to have a representation number for each sub-figures.

Information Disclosure Statement PTO-1449

5. The Information Disclosure Statement submitted by applicant on 01/09/2003 and 04/07/2003 (paper number 2 and 3) has been considered. Please see attached PTO-1449.

Claim Objections

6. **Claims 1-20** are objected to because of the following informalities: typo error.

Examiner suggests the following corrections:

Claim 1:

- insert phrase "password" after the phrase "from the" line 12 in order to change the phrase "from the database" to –from the password database--.

Claims 2-8,10 and 12-20:

- Replacement of phrase "a" (line 1, first occurrence) with "the".

Claim 9:

- add the phrase "identifier" after the phrase "the secure password" line 8.
- Replacement of phrase "the" (line 10, second occurrence) with "a".

Claim 11:

- Replacement of phrase "a" (line 3, second occurrence) with "the".

Claims 12-20:

- Replacement of phrase "a" (line 1, second occurrence) with "the".

Claims 15, 17 and 18:

- Replacement of phrase "a" line 2 with "the".

Claim 20:

- Replacement of phrase "a" line 3, second and third occurrences) with the phrase "the first".

Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the language of the claims or any helpful clarifications in that respect.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

8. **Claims 7 and 8** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

9. **Claim 7** recites the limitation "the protected file" in line 3 of the claim. There is insufficient antecedent basis for this limitation in the claim.

10. **Claim 8** recites the limitation "the protected file" in line 2 of the claim. There is insufficient antecedent basis for this limitation in the claim.

- Examiner considers the protected file as a file that corresponds access condition using password or key or identifier, etc. for the purpose of examination.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. **Claims 1-4 and 6-10** are rejected under 35 U.S.C. 103(a) as being unpatentable over He (5,944,824 A) in view of Brown et al (6,618,806 B1).

As per claim 1 He (5,944,824 A) teach a method of providing improved security for systems or files accessible by password data entry **(see col.2, lines 25-28 where a method of accessibility of a system using password that addresses the security of the system is disclosed)** comprising the steps of: determining a secure password **(see col.2, lines 36-39 where determination of a secure password is being processed either by initiation, modification and recovery of a password in a protected manner)**; providing a system or file **(see fig.7, items 12 disclose a user system where a user communicate with a network 10; col.2, lines 25-28 disclose a system)**; providing the secure password to a password database independent of the

system **(see fig.7 where the database 13 of security server 15 is independent of user system 12; col.10, lines 37-40 disclose database of 13 is located within the security server 15; col.9, lines 29-31 disclose passwords are stored in the security server database where the database 13 corresponds to password database of Applicant; col.10, lines 42-54 disclose the records of user accounts store in the database 13 contains field such as present password or new password)** and the file for storage therein in association with a security level **(see col.1, lines 23-30 where NEs are described as switches, databases and other network resources. Examiner considers other network resources corresponds to Applicant's file since file is a resource and see fig.2, item 58 where user access privilege control corresponds to Applicant's security level of a user; col.4, lines 12-19 where based on access privileges the information retrieved from database are disclosed; Also col.5, lines 41-48 disclose the access right based on the user privilege; therefore file stored are associated with user access privilege or security level)**; providing the secure password to a password sub-system for securing the determined system or file **(see fig.4, item 79, 84, 88 and 98; col.8, lines 9-15 disclose determining a secure password for entry subsystem NEs)**; when the individual is authorized **(see fig.5, item 104 where user is authenticated)**, retrieving the secure password from the database **(see fig.4, item 92 where retrieve user's password for accessing reasons are being done by recovery procedure that could be manual or automatic)** and automatically providing the secure password to the system or file password subsystem for accessing the system or file **(see fig.4, item**

79, 84 and 86, 96 where the password generation and recovery or retrieving may be automatic and secure since it is protected) wherein the system or file is accessible by manually entering the secure password to the password sub-system **(see fig.13, item 356; col.5, lines 7-9 where user enters information consist of a password and user identifiers; col.8, lines 28-32 disclose user originally did a log-on)** but do not disclose explicitly determining a user authorization method having an associated security level sufficient for accessing the secure password; authorizing an individual according to the secure authorization method. **However** Brown et al (6,618,806 B1) disclose determining a user authorization method having an associated security level sufficient for accessing the secure password **(see col.5, lines 5-29 where based on different set of instructions that corresponds to Applicant's associated security level a different biometric challenge being conducted that corresponds to Applicant's different methods and if verified the secure password is being retrieved for access)**; authorizing an individual according to the secure authorization method **(see col.5, lines 5-29 where based on the verification of biometric challenge authorization is being done by verification; col.8, lines 37-65 details the different authorization method or authentication)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Brown's biometric authorization methods that corresponds to different rules based on different instructions where the biometric information's are stored in the database in He's single sign-on NEs databases method of access authentication in order to provide an

authentication rule associated with a user based on different parameters of biometric data of a user.

As per claim 2 He (5,944,824 A) teach the method of providing improved security for systems or files accessible by password data entry as defined in claim 1 wherein the step of determining the secure password comprises the step of automatically determining the secure password **(see fig.4, item 79, 84 and 86 and also item 96 where the password generation may be automatic and secure since it is protected; col.8, lines 13-14 disclose password generation is done by automatic selection)**.

As per claim 3 He (5,944,824 A) teach the method of providing improved security for systems or files accessible by password data entry as defined in claim 2 wherein the determined secure password is secret and remains inaccessible to users of the system **(see col.7, lines 64-67 where it disclose that the password for the user does not have to be known to the user and therefore it can be a secure and inaccessible; col.9, lines 33-44 disclose detailed)**.

As per claim 4 He (5,944,824 A) teach the method of providing improved security for systems or files accessible by password data entry as defined in claim 1 wherein the password database comprises a key data file **(see col.9, lines 29-32 where examiner**

considers the user identifier as a key data file used for authentication in order to give access to the data).

As per claim 6 He (5,944,824 A) teach the method of providing improved security for systems or files accessible by password data entry as defined in claim 1 wherein the step of determining the secure password comprises the steps of manually providing the secure password to a password entry sub system **(see fig.4, item 79, 84, 88 and 98; col.8, lines9 and 16-18 disclose determining a secure password manually for entry subsystem NEs)**; and recording the password during entry **(see col.9, lines 50-54 where the act of log-on using the password corresponds to Applicant's recording of the password during entry)**.

As per claim 7 He (5,944,824 A) teach the method of providing improved security for systems or files accessible by password data entry as defined in claim 1 wherein the password is stored in association with data indicative of the protected file **(see col.9, lines 29-32 where password stored with user identifiers where the user identifiers are data indicative of the protected file since in col.5, lines 7-13 disclose the identifiers are user's information where upon authentication access is granted to NE's protected data)**.

As per claim 8 He (5,944,824 A) teach the method of providing improved security for systems or files accessible by password data entry as defined in claim 1 wherein the

protected file is stored in association with data indicative of the password **(see col.9, lines 29-32 where the user identifiers that are data corresponding to protected files or data of NEs which also are indicative of the identifiers corresponding password)**.

As per claim 9 He (5,944,824 A) teach a method of providing improved security for files accessible by password data entry **(see col.2, lines 25-28 where a method of accessibility of a system using password that addresses the security of the system is disclosed)** comprising the steps of: selecting a secured data file **(see col.1, lines 23-30 where NEs are described as switches, databases and other network resources. Examiner considers other network resources corresponds to Applicant's secure data file since secure data file is a resource; fig.12, item 312-322 disclose the process of returning the list of NEs or secure files, item 324 disclose selection of the user from the list and therefore selecting the NE user request access as depicted in item 326)**; providing a password database **(see col.10, lines 37-40 disclose database of 13 is located within the security server 15; col.9, lines 29-31 disclose passwords are stored in the security server database where the database 13 corresponds to password database of Applicant; col.10, lines 42-54 disclose the records of user accounts store in the database 13 contains field such as present password or new password)**; when the individual is authorized **(see fig.5, item 104 where user is authenticated)**, retrieving the secure password from the database **(see fig.4, item 92 where retrieve user's password for accessing reasons**

are being done by recovery procedure that could be manual or automatic) and automatically providing the secure password to the selected secured file password entry subsystem **(see fig.4, item 79, 84, 88 and 98; col.8, lines 9-15 disclose determining a secure password for entry subsystem NEs and item 79, 84 and 86, 96 where the password generation and recovery or retrieving may be automatic and secure since it is protected)**; automatically determining a secure password identifier associated with the secured data file **(see item 312 of fig.12 where passwords corresponding to NEs or secure files and user accounts are created; col.14, lines 44-47 disclose the log-on procedure is automatic and therefore such association is determined automatically)** but do not explicitly determining a user authorization method having an associated security level sufficient for accessing the secure password; authorizing an individual according to the secure authorization method. However Brown et al (6,618,806 B1) teach determining a user authorization method having an associated security level sufficient for accessing the secure password; authorizing an individual according to the secure authorization method **(see col.5, lines 5-29 where based on different set of instructions that corresponds to Applicant's associated security level a different biometric challenge being conducted that corresponds to Applicant's different methods and if verified the secure password is being retrieved for access)**; authorizing an individual according to the secure authorization method **(see col.5, lines 5-29 where based on the verification of biometric challenge authorization is being done by verification; col.8, lines 37-65 details the different authorization method or authentication)**. It would have been

obvious to one of ordinary skilled in the art at the time the invention was made to utilize Brown's biometric authorization methods that corresponds to different rules based on different instructions where the biometric information's are stored in the database in He's single sign-on NEs databases method of access authentication in order to provide an authentication rule associated with a user based on different parameters of biometric data of a user.

As per claim 10 He (5,944,824 A) teach the method of providing improved security for files accessible by password data entry as defined in claim 9 wherein the password database comprises a plurality of passwords **(see col.9, lines 29-30 disclose database stores passwords that corresponds to a plurality of password and col.4, lines 14-18 where it disclose databases)** and wherein the step of determining a secure password identifier comprises the step of determining a password from the plurality of passwords for use in accessing data within the secured data file **(see col.6, lines 13-23 disclose authorization uses an access control list for NEs entries by a user; col.5, lines 7-14 disclose based on selection of a password of a user and authentication access is being granted).**

13. **Claim 5** is rejected under 35 U.S.C. 103(a) as being unpatentable over He (5,944,824 A) in view of Brown et al (6,618,806 B1), and further in view of Eldridge et al (6,061,799 A).

As per claim 5 He (5,944,824 A) in view of Brown et al (6,618,806 B1) teach the method of providing improved security for systems or files accessible by password data entry as defined in claim 4 above but do not disclose explicitly the password database is stored within a portable storage medium. However Eldridge et al (6,061,799 A) teach a removable media for password based authentication in a distributed system where a password database is stored within a portable storage medium **(see fig.3A; col.1, lines 66-67 and cl.2, lines 1-5 where it disclose a database within a portable medium that contains authentication data including passwords)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Eldridge's portable medium password database in He's single sign-on NEs databases method of access authentication on authentication procedure in Brown's biometric authorization methods that corresponds to different rules based on different instructions where the biometric information's are stored in the database in order to provide an authentication rule associated with a user based on different parameters of biometric data of a user in order to update the security server process with the most current data during the authentication process by comparing the data stored in the server with the one in the portable medium.

Claim Rejections - 35 USC § 102

14. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

15. **Claims 11 and 15-19** are rejected under 35 U.S.C. 102(e) as being anticipated by Nielson (6,182,229 B1).

As per claim 11 Nielson (6,182,229 B1) teach a method of changing a first password for securing files accessible by password data entry comprising the steps of: determining a plurality of files secured with a first password **(see col.3, line67 and col.4, lines 1-2 where passwords within the database protect the remote server; col.3, lines 12-22 where a table with each entry of URL specifies the site access protocol and the name of the site where each URLs corresponds to plurality of files (please see definition of URL in a computer dictionary), and the encrypted password that corresponding to a url file as depicted in fig.2 corresponds to Applicant's first password that secure the file)** ; providing a second other password

for securing the plurality of files **(see col.3, lines 21-24 disclose a master password that being used to encrypt the passwords for the remote server entry and possibly the ids, this master password corresponds to the second password that protects security for the urls by encrypting the access password of url)**; for each file secured with the first password, accessing the file with the first password **(see fig.2 where the first password corresponds the url is used to access the web site once is decrypted, it also can be done manually or automatically)** and securing the file with the second other password **(see col.3, lines 21-24 disclose a master password that being used to encrypt the passwords for the remote server entry and possibly the ids, this master password corresponds to the second password that protects security for the urls that corresponds to files that are being secured)** ; storing the second other password in the password database **(see col.4, lines 34-36 where it disclose the master password that corresponds to Applicant's second password is stored in the memory; fig.3, item 312 and 314 disclose the master password or second password stored in the password database)**.

As per claim 15 Nielson (6,182,229 B1) teach the method of changing a first password for securing files accessible by password data entry as defined in claim 11 wherein the step of determining a plurality of files secured with the first password comprises the step of determining from the password database, files associated with the first password **(see col.3, line67 and col.4, lines 1-2 where passwords within the database protect the remote server; col.3, lines 12-22 where a table with each entry of URL**

specifies the site access protocol and the name of the site where each URLs corresponds to plurality of secure files and the encrypted password corresponding to a url file as depicted in fig.2 corresponds to Applicant's first password).

As per claim 16 Nielson (6,182,229 B1) teach the method of changing a first password for securing files accessible by password data entry as defined in claim 15 wherein those files associated with the first password are identified because they are identified by an identifier associated with the first password **(see fig.2 where user id associate with their corresponding password and file url; col.3, lines 48-53 where the association with controlled web site or a page. Examiner has considered address of secure web site URL as a file that need password for access since url address could corresponds to a particular file for access).**

As per claim 17 Nielson (6,182,229 B1) teach the method of changing a first password for securing files accessible by password data entry as defined in claim 11 wherein the step of determining a plurality of files secured with the first password comprises the step of determining from accessible files, those files associated with the first password **(see fig.2 where user id associate with their corresponding password and file url; col.3, lines 48-53 where the association with controlled web site or a page. Examiner has considered address of secure web site URL as a file that need password for access since url address could corresponds to a particular file for**

access and they are secure since the password and possibly user IDs are encrypted as depicted in fig.2).

As per claim 18 Nielson (6,182,229 B1) teach the method of changing a first password for securing files accessible by password data entry as defined in claim 11 wherein the step of providing a second other password includes the step of automatically generating the second other password **(see col.5, lines 555-61 where it disclose passwords can be generated automatically by password management).**

As per claim 19 Nielson (6,182,229 B1) teach the method of changing a first password for securing files accessible by password data entry as defined in claim 18 wherein the method of changing first password is automatically repeated at intervals **(see col.19-20 where it disclose the password particular to specific site (URL address (file) could be random for enhancing the security where such password corresponds to Applicant's first password as detailed in claim 11 above).**

16. **Claims 12, 13 and 20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Nielson (6,182,229 B1) in view of Bellemore et al (6,145,086 A).

As per claim 12 Nielson (6,182,229 B1) teach all limitation of the claim but do not explicitly disclose the step of changing password includes: archiving the first password for use in accessing archival files secured with the first password. However Bellemore

et al (6,145,086 A) disclose security and password mechanism with relationship to a database where the process of changing a password includes archiving the password as old password **(see col.5, lines 23-27 where it disclose history table contains used password as also depicted in fig.5, item 209)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Bellemore et al's history table in Neilson's password database in order to archive old passwords for approval of new password and by comparison means to be sure the new password does not be the same as last N old passwords.

As per claim 13 Nielson (6,182,229 B1) teach all limitation of the claim but do not explicitly disclose the step of authorizing an individual requesting a change of the first password prior to changing the first password. However Bellemore et al (6,145,086 A) disclose the step of authorizing an individual requesting a change of the first password prior to changing the first password **(see col.6, lines 58-63 where the request for change of password is being done by client that corresponds to Applicant's individual)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Bellemore et al's history table and password change request in Neilson's password database security method in order to determine whether the proposed password may be used as a password by archive old passwords for approval of new password and by comparison means to be sure the new password does not be the same as last N old passwords .

As per claim 20 Nielson (6,182,229 B1) teach the method of changing first password is automatically repeated at intervals **(see col.19-20 where it disclose the password particular to specific site (URL address (file) could be random for enhancing the security where such password corresponds to Applicant's first password as detailed in claim 11 above)** but do not disclose explicitly changing the password is repeated upon detection of a breach of a password and upon expiry of a password. However Bellemore et al (6,145,086 A) disclose the method of automatically changing the password is repeated upon detection of a breach of a password and upon expiry of a password **(see fig.3, item 310, 314 and 318 where determination is made for breach of a password by monitoring the number of failed attempt; item 360, 370 and 328 in fig.3 represent the expiry of password monitoring)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Bellemore et al's history table and password change rules in Neilson's password database automatic password generation security method in order to invoke a security process in response to client transmission of a connection message to the database management.

17. **Claim 14** is rejected under 35 U.S.C. 103(a) as being unpatentable over Nielson (6,182,229 B1) in view of Bellemore et al (6,145,086 A) and further in view of Brown et al (6,618,806 B1).

As per claim 14 Nielson (6,182,229 B1) teach all limitation of the claim as applied in claim 13 above but do not explicitly disclose the steps of: determining a user authorization method having an associated security level sufficient for accessing the secure password; and, authorizing an individual according to the secure authorization method. However Brown et al (6,618,806 B1) teach determining a user authorization method having an associated security level sufficient for accessing the secure password; authorizing an individual according to the secure authorization method **(see col.5, lines 5-29 where based on different set of instructions that corresponds to Applicant's associated security level a different biometric challenge being conducted that corresponds to Applicant's different methods and if verified the secure password is being retrieved for access)**; authorizing an individual according to the secure authorization method **(see col.5, lines 5-29 where based on the verification of biometric challenge authorization is being done by verification; col.8, lines 37-65 details the different authorization method or authentication)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Brown's biometric authorization methods that corresponds to different rules based on different instructions (different security level authorization method) where the biometric information's are stored in the database in Neilson's password database automatic password generation security method in order to provide an authentication rule (method) associated with a user based on different parameters of biometric data of a user and further in view of Bellemore et al's history table and password change request in order to determine whether the proposed password may

be used as a password by archive old passwords for approval of new password and by comparison means to be sure the new password does not be the same as last N old passwords .

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

a. U.S.Patent No. US (5,889,860 A) teach encryption system with transaction coded decryption key.

b. U.S.Patent No. US (6,343,284 B1) teach method and system for billing on the Internet.

c. U.S.Patent No. US (6,618,806 B1) teach system and method for authenticating users in a computer network.

d. U.S.Patent No. US (5,495,533 A) teach personal key archive.

e. U.S.Patent No. US (6,609,115 B1) teach method and apparatus for limited online access to restricted documentation.

f. U.S.Patent No. US (5,862,323 A) teach retrieving plain-text passwords from a main registry by a plurality of foreign registries.

g. U.S.Patent No. US (5,944,824 A) teach system and method for single sign-on to a plurality of network elements.

h. U.S.Patent No. US (6,108,790 A) teach authentication system using network.

i. U.S.Patent No. US (6,584,454 B1) teach method and apparatus for community management in remote system serving.

j. U.S.Patent No. US (6,351,813 B1) teach access control/crypto system

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (703) 306-4169. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

08/18/04